---

layout: page

title:"நான் கண்காணிக்கப்படுகிறேன் என்று நினைக்கிறேன்"

author: Carlos Guerra, Peter Steudtner, Ahmad Gharbeia

language: en

summary: " இந்த பனிப்பாய்வானது நீங்கள் டிஜிட்டல் கண்காணிப்பின் இலக்காக இருக்கலாம் நீங்கள் எண்ணினால், கண்காணிப்னுடைய சாத்தியமான குறிகாட்டிகளை அடையாளம் காண கேள்விகளினூடாக வழிகாட்டும்."

date: 2023-05

permalink: /en/topics/surveilled

parent: Home

---

# நான் கண்காணிக்கப்படுகிறேன் என்று நினைக்கிறேன்

சிவில் செயற்பாட்டாளர்கள் மீதான கண்காணிப்பு தொடர்பான முறைப்பாடுகளானது அதிகரிப்பதனை காணக்கூடியதாகவுள்ளது. தவறானவர்களின் ஒன்றிணைந்த பின்தொடர்தல் மற்றும் ஊழியர்களின் தொழில் முறையான கண்காணிப்பு, தொடக்கம் வெகுஜன அரசு கண்காணிப்பு மற்றும் ஆர்வலர்கள் மற்றும் பத்திரிகையாளர்களுக்கு எதிரான வேவுபார்க்கும் பிரச்சாரங்கள் வரை பல வளர்ந்து வரும் நிகழ்வுகளை நாங்கள் காணக்கூடியதாகவுள்ளது. அவதானிக்கப்பட்டதன் அடிப்படையில் கண்காணிப்பின் அத்தனை முறைகளினையும் குறிப்பாக அவசர உதவி வழங்குதலில் உள்ளடக்க முடியாது .

இந்த பணிப்பாய்வானது டிஜிட்டல் பரப்பில் காணப்படும் பொதுவான நிகழ்வுகளில் கவனம் செலுத்துவதுடன், இறுதிப் பயனர் சாதனங்கள் மற்றும் நிகழ்நிலைக் கணக்குகளுடன் தொடர்புடைய பொதுவான சந்தர்ப்பங்களை மையமாகக் கொண்டு, உடனடியாக நடவடிக்கை எடுக்க வேண்டிய அவசரமான சந்தர்பங்களுடன் தொடர்புபட்டது. சாத்தியமான தீர்வு ஓன்று காணப்படாதபோது அவை அவசர நிலையாகக் கருதப்பட மாட்டாது மற்றும் அவை விரிவாக நோக்கப்பட மாட்டாது. (அதற்கு பதிலாக, உசாத்துணைகள் பகிரப்படும்).

இந்த பணிப்பாய்வில் உள்ளடக்கப்படாத சில பிரச்சினைகள் :

- பௌதீக கண்காணிப்பு மூலம் நீங்கள் இலக்கு வைக்கப்படுவீர்கள் என்று நீங்கள் அஞ்சினால் மற்றும் உதவியினைப் பெற விரும்பினால், டிஜிட்டல் முதலுதவி பொதியின் [ஆதரவு பக்கம்](../../support) பௌதீக பாதுகாப்பில் கவனம் செலுத்தும் நிறுவனங்களை நீங்கள் அணுகலாம்.

- பொதுவிடங்களில் , வேலைத்தளங்களில் மற்றும் தனியார் இடங்களில் கண்காணிப்புக் கேமராக்கள் போன்ற வன்பொருள் மூலம் பாரிய கண்காணிப்பு செய்தல்.

- வன்பொருள் பிழைகள் இணையத்தில் தங்கியிருப்பதல்ல.

இரண்டாவது பொருத்தமான பொறுப்புத்துரைப்பு யாதெனில், நவீன நாட்களில் அனைவரும் ஏதோ ஒரு வகையில் இயல்பாகவே கண்காணிக்கப்படுகிறார்கள்:

- கையடக்கத் தொலைபேசியினுடைய உட்கட்டமைப்பானது எம்மைப்பற்றிய ஏராளமான தகவலினை சேமிக்கக்கூடிய வகையில் அமைக்கப்பட்டுள்ளது. இவை எமது அமைவிடம், தொடர்புகள் வலையமைப்பு என்பவற்றினை அறிந்துகொள்ள பல்வேறு செயற்பாட்டாளர்களால் பயன்படுத்தப்படலாம்.

- சமூக வலையமைப்புகள் மற்றும் மின்னஞ்சல் வழங்குநர்கள் போன்ற ஒன்லைன் சேவைகள் எம்மைப்பற்றிய ஏராளமான தகவல்களினைச் சேமிக்கின்றன. உதாரணமாக எங்கள் இடுகைகளின் தலைப்புகள் அல்லது ஒருவருக்கு ஒருவர் பரிமாறிக்கொள்ளும் செய்திகள் தொடர்பான விளம்பரங்களைக் காட்ட விளம்பர பிரச்சாரங்களுடன் இணைக்கலாம்.

- அதிகமான நாடுகளில் பல ஒன்றிணைந்த அமைப்புகள் காணப்படுகின்றன, அவர்கள் எமது அடையாளங்களினை பயன்படுத்துவதுதான் பல்வேறுபட்ட பொது அமைப்புகளுடனான எமது தொடர்பாடல்களினையும் சேமித்துவரி அல்லது ஆரோக்கியம் தொடர்பான தகவலுக்கான ஆவணக் கோரிக்கைகளின் அடிப்படையில் "சுயவிவரத்தை" உருவாக்க உதவுகிறது.

பொதுஜன கண்காணிப்பின் இந்த உதாரணகள் மற்றும் இலக்கு நடவடிக்கைகளின் பல முன்னைய செயற்பாடுகள், போன்றவை அனைவரும் (குறிப்பாக ஆர்வலர் இடத்தில்) கண்காணிக்கப்படுவதான ஒரு உணர்வினை உருவாக்குகின்றது, இது உளவியல் தாக்கங்களுக்கு உட்படுத்துவதுடன் உண்மையான அச்சறுத்தல்களுடன் போராடுவதற்கான எமது திறனைப் பாதிக்கும். அதாவது, குறிப்பிட்ட நிகழ்வுகள் உள்ளன - நமது ஆபத்து விவரம், நாம் செய்யும் வேலை மற்றும் நமது சாத்தியமான எதிரிகளின் திறன் ஆகியவற்றைப் பொறுத்து - நாம் கண்காணிக்கப்படுகிறோம் என்ற சந்தேகத்தை நாங்கள் நிறுவியிருக்கலாம். உங்களது விடயத்திலும் அவ்வாறு காணப்படின் தொடர்ந்தும் படியுங்கள்.

மூன்றாவது பொறுப்புத் துறப்பு, பல கண்காணிப்புத் திட்டங்களானவை (குறிப்பாக இலக்கு வைக்கப்பட்டவை), பாதிப்படைந்தவர்களினால் அணுகப்படக்கூடிய சில அல்லது எந்த குறிகாட்டிகளையும் விட்டுச்செல்வதில்லை, இது கண்டுபிடிப்பதை கடினமாகும் அல்லது சாத்தியமற்றதாக்குகின்றது. பணிப்பாய்வினை செய்யும்போது இதைக் கவனத்தில் கொள்ளவும், உங்கள் பிரச்சினையானது இன்னும் சிக்கலானதாகவோ அல்லது உள்ளடக்கப்படவில்லையென நீங்கள் நம்பினால், பணிப்பாய்வு முடிவில் பட்டியலிடப்பட்டுள்ள நிறுவனங்களைத் தொடர்பு கொள்ளவும்.

இறுதியான விடயமாக, கண்காணிப்பு முயற்சிகள் மிகப்பெரியதாகவோ அல்லது குறிவைக்கப்பட்டதாகவோ காணப்படலாம் என்பதனை நினைவில் கொள்ளவும். பாரிய கண்காணிப்பு நடவடிக்கைகள் பொதுவாக முழு மக்கள்தொகை அல்லது அவர்களின் பெரிய பகுதிகளை உள்ளடக்கும், ஒரு தளத்தினை பயன்படுத்துகின்ற அனைவரும், ஒரு குறிப்பிட்ட பகுதியைச் சேர்ந்தவர்கள் போன்றவற்றினை உள்ளடக்கும் . இவை பொதுவாக தொழில்நுட்பத்தில் அதிகம் தங்கியிருக்கும் மற்றும் ஓன்று அல்லது சிறிய எண்ணிக்கையிலான நபர்களை இலக்கு வைக்கும், பிரத்தியேகமான வழங்களைக்கொண்ட (பணம், நேரம் மற்றும்/அல்லது திறன்) குறிவைக்கப்பட்ட கண்காணிப்புடன் ஒப்பிடுகையில் ஆபத்து குறைந்தவை. மேலும் குறிப்பிட்ட நபர்களின் செயல்பாடு மற்றும் தகவல்தொடர்புகளைக் கண்காணிக்க ஆதாரங்களை வைப்பதன் பின்னணியில் உள்ள உந்துதல்களைக் காட்டிலும் பாரிய கண்காணிப்பை விட பொதுவாக மிகவும் ஆபத்தானது.

நீங்கள் கண்காணிக்கப்படுகிறீர்கள் என்பதற்கான அறிகுறிகளினைக் கண்டறிந்தால், பணிப்பாய்வு தொடங்குவதற்குத் STARTஎன்பதைக் கிளிக் செய்யவும்.

## பணிப்பாய்வு

### தொடக்கம்

> நீங்கள் இங்கே இருந்தால், உங்கள் தகவல்தொடர்புகள், இருப்பிடம் அல்லது பிற ஆன்லைன் செயல்பாடுகள் கண்காணிக்கப்படலாம் என்று நினைக்க உங்களுக்கு காரணங்கள் காணப்படலாம். கண்காணிப்பு தொடர்பான சந்தேகத்திற்கிடமான செயல்பாட்டின் பொதுவான குறிகாட்டிகளின் வரிசையை கீழே காணலாம். தொடர்வதற்கு உங்களது பிரச்சினையினை அழுத்துங்கள்.

அறிமுகத்தில் கொடுக்கப்பட்டுள்ள தகவல்களின்படி, நீங்கள் என்ன மாதிரியான சிக்கலைச் சந்திக்கிறீர்கள்?

- [எனக்கு அருகில் ஒரு கண்காணிப்பு சாதனத்தைக் கண்டேன்](#tracking-device-intro)

- [எனது சாதனம் சந்தேகத்திற்கிடமான முறையில் செயல்படுகிறது](#device-behaviour-intro)

- [புதுப்பிப்புகள் அல்லது பயன்பாடுகளை நிறுவுவதற்காக நான் பாதுகாப்பற்ற http-இணையதளங்களுக்குத் திசைதிருப்பிவிடப்படுகிறேன்](#suspicious-redirections-intro)

- [நம்பகமான சேவைகளிலிருந்து பாதுகாப்புச் செய்திகள் மற்றும் விழிப்பூட்டல்களைப் பெறுகிறேன்](#security-alerts-intro)

- [எனது கணினி அல்லது நெட்வொர்க்குடன் சந்தேகத்திற்கிடமான சாதனம் இணைக்கப்பட்டுள்ளது](#suspicious-device-intro)

- [மின்னஞ்சல், தூதுவர் அல்லது அதைப் போன்றது மூலம் நான் தனிப்பட்ட முறையில் பகிர்ந்து கொண்ட தகவல் எதிரிக்குத் தெரியும்](#லீக்-இன்டர்நெட்-இன்போ-அறிமுகம்)

- [சிதொலைபேசி அழைப்புகள் அல்லது எஸ்எம்எஸ் மூலம் பகிரப்படும் ரகசியத் தகவல்கள் எதிரிக்கு கசிந்ததாகத் தெரிகிறது (குறிப்பாக முக்கியமான நிகழ்வுகளின் போது)](#லீக்-ஃபோன்-இன்போ-அறிமுகம்)

- [உங்களைச் சுற்றியுள்ளவர்கள் கண்காணிப்பு நடவடிக்கைகளால் வெற்றிகரமாக இலக்கு வைக்கப்பட்டுள்ளனர்](#peer-compromised-intro)

- [வேறு ஒன்று / எனக்குத் தெரியாது](#மற்ற அறிமுகம்)

### கண்காணிப்பு-சாதனம்-அறிமுகம்

> உங்களுக்கு அருகில் எதிர்பாராத சாதனம் இருப்பதைக் கண்டறிந்து, அது ஒரு கண்காணிப்புச் சாதனம் என்று நீங்கள் நம்பினால், முதல் படியாக, சாதனம் உங்களைக் கண்காணிக்க உள்ளது என்பதை உறுதிப்படுத்துகிறது, மேலும் அது பிற தொடர்புடைய செயல்பாடுகளைச் செய்யாது. பொருட்களினுடைய இணையம் (Internet of Things)(IoT) சாதனங்களின் அறிமுகத்துடன், சிறிது நேரம் பயன்படுத்திய பிறகு நாம் மறந்துவிடக்கூடிய பெரிய அளவிலான செயல்களைச் செய்யும் சாதனங்களைக் கண்டுபிடிப்பது மிகவும் பொதுவானது. இது ஒரு கண்காணிப்பு சாதனம் என்பதை உறுதிசெய்வதற்கான முதல் படிகளில் ஒன்று, அதனது உற்பத்தி பெயர், உற்பத்தி மாதிரி போன்றவற்றினைக் கண்டறிய குறித்த சாதனத்தை சோதித்தல், சந்தையிலுள்ள விலை குறைந்த பொதுவான உற்பத்திகளாக Apple Airtags, Samsung Galaxy SmartTag அல்லது Tile போன்றவை காணப்படும். இவை சட்டபூர்வமான நடவடிக்கைகளுக்காக விற்கப்படுகின்றன. எனினும் மோசடிக்காரர்கள் மாதவர்களை அனுமதியின்றி கண்காணிப்பதற்காக துஸ்பிரயோகம் செய்யலாம்.

>

> எதிர்பாராத கண்காணிப்புக்கள் காணப்படுகின்றதா என்பதனை உறுதிப்படுத்த போதிக்க ரீதியாக அவற்றினை கண்டறிவதுடன் சில குறிப்பிட்ட தீர்வுகளை கருத்தில் கொள்ளுதல் வேண்டும்:

>

> - Apple Airtagsக்கு, iOS இல் [தெரியாத சாதனம் சில நேரம் கண்டறியப்பட்ட பிறகு, நீங்கள் ஒரு தானியங்கி அறிவிப்பைப் பெறுவீர்கள்](https://support.apple.com/en-us/HT212227).

> - ஆண்ட்ராய்டுக்கு, [அருகில் உள்ள ஏர்டேக்குகளைச் சரிபார்க்க ஆப்ஸ்](https://play.google.com/store/apps/details?id=com.apple.trackerdetect) உள்ளது.

> - டைல் சாதனங்களுக்கு, [Tile app](https://www.tile.com/download) தெரியாத டிராக்கர்களை சரிபார்க்கும் அம்சம் உள்ளது.

> - Samsung Galaxy SmartTagsக்கு, இதே அம்சத்திற்கு [SmartThings பயன்பாட்டை](https://www.samsung.com/us/smartthings/) பயன்படுத்தலாம்.

>

> நீங்கள் காணக்கூடிய மற்றொரு வகையான சாதனம் ஜிபிஎஸ்கருவிகளாகும். இவை இலக்குவைக்கப்பட்டவரின் இருப்பிடத்தினை அடிக்கடி வழங்குவதுடன் இவை தொலைபேசியூடாக வழங்குகின்றது அல்லது பின்னர் சேகரிக்கக்கூடிய வகையில் ஏதாவது ஒரு இடத்தில் சேமிக்கின்றது. இதுபோன்ற சாதனத்தை நீங்கள் கண்டால், சாதனம் செயல்படும் விதத்தைப் விளங்கிக்கொள்ளுதல், சாதனத்தை யார் நிறுவினார்கள் மற்றும் அவர்கள் எவ்வாறு தகவலைப் பெறுகிறார்கள் என்பதைப் பற்றிய சிறந்த தகவல்களினைப் பெறுவதற்கு முக்கியமாகும்.

>

> நீங்கள் கண்டுபிடிக்கும் எந்த வகையான கண்காணிப்பு சாதனத்திற்கும், அதைப் பற்றிய அனைத்தையும் ஆவணப்படுத்த வேண்டும்: எந்த உற்பத்தி, உட்பத்தி மாடல், மின்கம்பியற்ற வலையமைப்புடன் இணைக்கப்பட்டால், அதை நீங்கள் சரியாகக் கண்டறிந்த இடம், தொடர்புடைய பயன்பாட்டில் உள்ள சாதனத்தின் பெயர்கள் போன்றவற்றினை ஆவணப்படுத்தல் வேண்டும்.

சாதனத்தை அடையாளம் கண்ட பிறகு, நீங்கள் பின்பற்ற விரும்பும் சில உத்திகள் உள்ளன. சாதனத்தை என்ன செய்ய விரும்புகிறீர்கள்?

- [நான் அதை முடக்க விரும்புகிறேன்](#tracking-disable-device)

- [இயக்குபவரைத் தவறாக வழிநடத்த இதைப் பயன்படுத்த விரும்புகிறேன்](#டிராக்கிங்-யூஸ்-டிவைஸ்)

### கண்காணிப்பு-முடக்குதல் -சாதனம்

> நீங்கள் கண்டறிந்த சாதனத்தின் வகை மற்றும் உற்பத்திவகையினை பொறுத்து, நீங்கள் அதை நிறுத்திவைக்கலாம் அல்லது முழுவதுமாக முடக்கலாம். சில சந்தர்ப்பங்களில், முந்தைய படியில் விவரிக்கப்பட்டதைப் போன்ற கண்காணிப்புச் செயலிகள் மூலமாகவும், பௌதீக சக்தி ஆளிகள் மூலமாகவும் அல்லது சாதனத்தை சிதைப்பதன்மூலமாகவும் இதைச் செய்யலாம். இந்தச் சம்பவத்தைப் பற்றி நீங்கள் ஆழமான விசாரணையை நடத்த விரும்பினால், சாதனத்தை முடக்குவது, சாதனத்தில் சேமிக்கப்பட்டுள்ள தொடர்புடைய ஆதாரங்களை மாற்றக்கூடும் என்பதை நினைவில் கொள்ளவும்.

சாதனத்தின் உரிமையாளரைக் கண்டறிய மேலும் நடவடிக்கை எடுக்க விரும்புகிறீர்களா? (\*அவ்வாறு செய்ய கண்காணிப்பு சாதனத்தை நிகழ்நிலையில் வைத்திருக்க வேண்டும் என்பதை நினைவில் கொள்ளவும்\*)

- [ஆம்](#சாதன உரிமையாளரை அடையாளம் காணவும்)

- [இல்லை](#முன் மூடுதல்)

### கண்காணிப்பு-பயன்பாட்டு-சாதனம்

>கண்காணிப்பு சாதனைகளை கையாள்வதற்கான சிறப்பான வழிமுறையிலொன்று அவை கண்காணிக்க எண்ணிய விடயத்தை விட வேறொன்றை கண்காணிக்கச் செய்தலாகும். உதாரணாமாக நீங்கள் வேறு இடங்களுக்கு செல்லும்போது அதனை நிலையான ஒரு இடத்தில் வைத்தால் அல்லது அதனது கண்காணிப்பினை வேறு விடயத்துக்கு திருப்புதல் போன்றவை. . இந்தக் காட்சிகளில் சிலவற்றில் நீங்கள் சாதனத்திற்கான அணுகலை இழக்க நேரிடலாம் மற்றும் கண்காணிப்பானானது வேறொரு நபரைப் பின்தொடரச் செய்வது அல்லது குறிப்பிட்ட இருப்பிடத்தைக் கண்காணிப்பது பாதுகாப்பு மற்றும் சட்டரீதியான தாக்கங்களைக் கொண்டிருக்கலாம் என்பதை நினைவில் கொள்ளவும்.

சாதனத்தின் உரிமையாளரைக் கண்டறிய மேலும் நடவடிக்கை எடுக்க விரும்புகிறீர்களா? (\*அவ்வாறு செய்ய கண்காணிப்பு சாதனத்தை ஆன்லைனில் வைத்திருக்க வேண்டும் என்பதை நினைவில் கொள்ளவும்\*)

- [ஆம்](#சாதன உரிமையாளரை அடையாளம் காணவும்)

- [இல்லை](#முன் மூடுதல்)

### -சாதன - உரிமையாளர்- அடையாளம் காணுதல்

> கண்காணிப்பு சாதனத்தின் உரிமையாளரைக் கண்டறிவது சில சந்தர்ப்பங்களில் கடினமாகலாம். இது சாதனத்தைப் பொறுத்து மாறுபடும் எனவே குறித்த சாதனம் தொடர்பான ஆய்வினை மேற்கொள்ள பரிந்துரைக்கப்படுகிறேர்கள். சில உதாரணங்கள்:

>

> - நுகர்வோர் தர வயர்லெஸ் டிராக்கர்களுக்கு:

> - உறுதிப்படுத்தல் செயலிகளில் அவை எவ்வாறு காட்டப்படுகின்றன?

> - நீங்கள் எப்போது அறிவிப்பைப் பெற்றீர்கள்?

> - தொடர்புடைய தகவலைக் கொண்டிருக்கும் சாதனத்திலிருந்து கூடுதல் தரவைப் பிரித்தெடுக்க ஏதேனும் வழி உள்ளதா?

> - GPS டிராக்கர்கள் போன்ற குறிப்பான கண்காணிப்பு சாதனங்களுக்கு:

> - அவற்றிடம் உள்ளக சேமிப்பு இருக்கிறதா? சில மாடல்களில் SD கார்டு உள்ளது, அது எப்போது டேட்டாவைப் பிடிக்கத் தொடங்கியது போன்ற அல்லது வேறு ஏதேனும் தொடர்புடைய தகவலைப் பிரித்தெடுக்கலாம்.

> - அத்துடன் தொலைபேசி இணைப்பு ஏதேனும் காணப்படுகின்றதா ? சாதனத்திலிருந்து சிம் அட்டையினை வேறுபிரித்து அதன் இலக்கத்தை தெரிந்துகொள்ள வேறொரு கைப்பேசியில் போடா இயலுமா? என சோதியுங்கள் இடந்தது தகவல்களைக் கொண்டு உருமையாளரினை அறிந்து கொள்ள முடியுமா?

> - பொதுவாக

> - சாதனத்தில் எழுதப்பட்ட பெயர்கள், பதிப்பு எண்கள் போன்ற ஏதேனும் இயற்பியல் குறிப்புகளைத் தேடுங்கள்.

> - சாதனம் இணையத்துடன் இணைக்கப்பட்டால், அடையாளம் தொடர்பான தகவலினைப் பெறக்கூடிய பெயர்கள் ஏதேனுமுண்டா?

> - நீங்கள் சாதனத்தைக் கண்டறிந்த இடத்தை யார் அணுக முடியும்? அது எப்போது பொறுத்தப்பட்டிருக்க முடியும்?

கண்காணிப்பு சாதன உரிமையாளருக்கு எதிராக சட்ட நடவடிக்கை எடுக்க விரும்புகிறீர்களா?

- [ஆம்](#சட்ட நடவடிக்கை-சாதன உரிமையாளர்)

- [இல்லை](#முன் மூடுதல்)

### சட்ட நடவடிக்கை-சாதன உரிமையாளர்

> கண்காணிப்பு சாதனத்தின் உரிமையாளருக்கு எதிராக நீங்கள் சட்ட நடவடிக்கை எடுக்க விரும்பினால், உங்கள் நியாயாதிக்க எல்லையில் எவ்வாறான நடைமுறைகள் காணப்படுகின்றது என்பதனை உறுதிப்படுத்திக்கொள்ளுதல் வேண்டும். |சில சந்தர்ப்பங்களில் ஒரு வழக்கறிஞர் தேவைப்படும், மற்றவற்றில், செயல்முறையைத் தொடங்க காவல் நிலையத்தை அணுகினால் போதுமானது. எல்லா வழக்குகளுக்கும் பொதுவான ஒரே அறிவுரை என்னவென்றால், எந்தவொரு வழக்கும் அதற்கு நீங்க சேமிக்கின்ற சான்றுகளின் வலுவினைப்போலவே வழக்கும் வலுவானதாக இருக்கும். இவற்றினை ஆவணப்படுத்துவது தொடர்பாக அறிந்துகொள்ள பனிப்பாய்வின் ஆரம்பப் பகுதிகளில் வழங்கப்பட்ட ஆலோசனைகளினை பின்பற்றுவது ஒரு நல்ல ஆரம்பமாகக் காணப்படும்.டிஜிட்டல் முதலுதவி பொதியில் [டிஜிட்டல் அவசரநிலைகளை ஆவணப்படுத்துதல்](/../../ஆவணம்) பற்றிய கூடுதல் தகவல்களையும் எடுத்துக்காட்டுகளையும் நீங்கள் காணலாம்.

கண்காணிப்பு சாதன உரிமையாளருக்கு எதிராக சட்ட நடவடிக்கை எடுக்க உங்களுக்கு உதவி தேவையா?

- [ஆம், எனக்கு சட்ட ஆதரவு தேவை](#சட்ட\_முடிவு)

- [இல்லை, எனது பிரச்சினைகளை நான் தீர்த்துவிட்டேன் என்று நினைக்கிறேன்](#தீர்ந்தது\_முடிவு)

- [இல்லை, ஆனால் நான் மற்ற கண்காணிப்பு காட்சிகளை பரிசீலிக்க விரும்புகிறேன்](#முன்-மூடுதல்)

### சாதனம்-நடத்தைக்கோலம் -அறிமுகம்

> இன்றுவரை மிகவும் பொதுவான இலக்கு கண்காணிப்பு நுட்பங்களில் ஒன்று, வேவுமென்பொருட்கள் மூலம் தொலைபேசிகள் அல்லது கணினிகளில் பாதிப்பை ஏற்படுத்துவதாகும் - தீம்பொருட்களானது செயல்பாட்டைக் கண்காணிக்கவும் மற்றவர்களுக்கு அனுப்பவும் வடிவமைக்கப்பட்டுள்ளது. பல்வேறுபட்ட செயற்பாட்டாளர்கள் வேவுமென்பொருளினை வேறுபட்ட வழிமுறைகளில் உதாரணமாக மோசடியான பங்காளர்கள் செயன்முறையாக உளவு மென்பொருள்களை பதிவிறக்கல் அல்லது தகவல் திருட்டு இணைப்புகளினை அனுப்பும் ஒழுங்கமைக்கப்பட்ட குற்றங்கள் போன்ற பல்வேறு வழிகளில் நிறுவிக்கொள்ள முடியும். (பொதுவாக ஸ்டால்கர்வேர் அல்லது ஸ்போஸ்வேர் என குறிப்பிடப்படுகிறது)

>

> கண்காணிப்பு குறிகாட்டிகளின் சில எடுத்துக்காட்டுகளில் மைக்ரோஃபோன், கேமரா, நெட்வொர்க் அணுகல் போன்றவற்றிற்கான அனுமதியுடன் உங்கள் சாதனத்தில் சந்தேகத்திற்குரிய பயன்பாடுகள் இருக்கலாம். வெப்கேம் காட்டி அதை இயக்க வேண்டிய எந்தப் பயன்பாட்டையும் பயன்படுத்தாமல் அல்லது சாதனத்தில் உள்ள கோப்புகளின் உள்ளடக்கத்தைப் பார்க்காமல் " கசிந்தது".

>

> இதுபோன்ற சந்தர்ப்பங்களில், டிஜிட்டல் முதலுதவி பொதியின் "எனது சாதனம் சந்தேகத்திற்கிடமான முறையில் செயல்படுகிறது" என்பதைப் பார்க்கவும்.

நீங்கள் என்ன செய்ய விரும்புகிறீர்கள்?

- [சந்தேகத்திற்கிடமான முறையில் செயல்படும் சாதனத்திற்கு என்னை அழைத்துச் செல்லுங்கள்](../../../device-acting-suspiciously)

- [இங்கே அடுத்த படிக்கு என்னை அழைத்துச் செல்லுங்கள்](#முன் மூடுதல்)

### சந்தேகத்திற்கிடமான திசைதிருப்பல்கள்-அறிமுகம்

> இவை வழமைக்கு மாறானவை ஆனாலும், சில சமயங்களில் நமது சாதனங்களில் செயலிகளை அல்லது இயந்திரத்தை புதுப்பிக்க முயற்சிக்கும்போது பாதுகாப்பு எச்சரிக்கைகள் காணப்படுகிறது. இதற்கான பல காரணங்கள் இருக்கலாம், அவை சட்டபூர்வமானதோ அல்லது தீங்கானதாகவோ ஆக இருக்கலாம். நாம் சிந்திக்க வேண்டிய சில வழிகாட்டி கேள்விகள் காணப்படுகின்றன :

>

> - என் சாதனத்தில் நேரம் மற்றும் தேதி சரியானதா? நமது சாதனங்கள் சரியான முறையில் செயற்படுவதனை உறுதிப்படுத்திக்கொள்ள , பாதுகாப்பு சான்றிதழ்களை பரிசீலிக்கின்றது, இது குறிப்பிட்ட கால வரையறைக்குள் செல்லுபடியாக காணப்படும். உதாரணமாக , உங்கள் கணினி பழைய ஆண்டில் அமைக்கப்பட்டிருந்தால், பல இணையதளங்களுக்கும் சேவைகளுக்கும் இந்த பாதுகாப்பு சரிபார்க்கைகள் தோல்வியடைந்துவிடும். உங்கள் தேதி மற்றும் நேரம் சரியானது என்றால், வழங்குபவர் தங்களின் சான்றிதழ்களை புதுப்பிக்கவில்லை அல்லது சந்தேகத்திற்குரிய ஒன்றுதான் நடக்கிறது என்பதைக் குறிக்கலாம். எதுவாயினும், இந்த பாதுகாப்பு எச்சரிக்கைகள் அல்லது மறுப்புகளை காணும் போது உங்கள் சாதனத்தில் செயலிகள் புதுப்பிக்க அல்லது இயக்காமல் இருப்பது ஒரு நல்ல செயல்முறையாகும்.

> - ஒரு அசாதாரண நிகழ்வுக்குப் பின்னர் இந்த பிரச்சனை ஏற்பட்டதா, உதாரணமாக, ஒரு விளம்பரத்தை கிளிக் செய்தல், ஒரு செயலியை நிறுவுதல் அல்லது ஒரு ஆவணத்தை திறப்பது? பலவிதமான தாக்குதல்கள் , சட்டபூர்வமான மென்பொருள் நிறுவல் மற்றும் புதுப்பிப்புகளை போன்ற போலியான மாறாட்டச் செயற்பாடுகளில் தங்கியுள்ளன. எனவே உங்கள் சாதனம் அதை கண்டறிந்து எச்சரிக்கையை வழங்கவோ அல்லது செயல்முறையை முழுமையாக நிறுத்தவோ செய்யலாம்.

> - வழக்கத்திற்கு மாறான முறையில் உங்களுக்குச் சிக்கல்கள் உள்ளதா, உதாரணம் : ஒரு செயலுக்கான புதுப்பித்தல் செயன்முறையானது வழமையான செயன்முறையிலும் பார்க்க பிறிதொரு முறையினை பின்பற்றுதல்?

>

> எவ்வாறாயினும், எல்லாவற்றையும் முடிந்தவரை விரிவான முறையில் ஆவணப்படுத்த மறக்காதீர்கள், குறிப்பாக நீங்கள் சிறப்பு உதவியைப் பெற விரும்பினால், ஆழமான விசாரணையை மேற்கொள்ள வேண்டும் அல்லது ஏதேனும் சட்ட நடவடிக்கை எடுக்க வேண்டும்.

>

> ஏறக்குறைய எல்லா நிகழ்வுகளிலும், சாதனம் மற்றும் வழிசெலுத்தலை இயல்பு நிலைக்குத் திரும்புவதற்கு முன், சிக்கலின் மூல காரணத்தை நிவர்த்தி செய்வது போதுமானதாக இருக்கும். இருப்பினும், சந்தேகத்திற்கிடமான சூழ்நிலையில் நீங்கள் உண்மையில் ஒரு பயன்பாட்டை (அல்லது இயக்க முறைமை) நிறுவியிருந்தால் அல்லது புதுப்பித்திருந்தால் மேலும் சிக்கல்கள் தோன்றலாம்.

சந்தேகத்திற்கிடமான நிபந்தனைகளுடன் ஏதேனும் மென்பொருள் அல்லது புதுப்பிப்புகளை கிளிக் செய்து பதிவிறக்கம் செய்தல் அல்லது மென்பொருளினை நிறுவல் செய்தீர்களா?

- [ஆம்](#முன்- மூடுதல்)

- [இல்லை](#சந்தேகத்திற்குரிய-மென்பொருள்-நிறுவப்பட்டது)

### சந்தேகத்திற்கிடமான மென்பொருள் நிறுவப்பட்டது

> பெரும்பாலான சந்தர்ப்பங்களில், செயலிகளினுடைய அல்லது இயக்க முறைமைகளின் நிறுவல் அல்லது புதுப்பித்தல் செயல்முறைகளை கைப்பற்றல் தாக்குதலானது கணினியில் தீம்பொருளை நிறுவுவதை நோக்கமாகக் கொண்டுள்ளன. இது தான் உங்களது நிலை என நீங்கள் சந்தேகித்தால், டிஜிட்டல் முதலுதவிப் பொதியின் "எனது சாதனம் சந்தேகத்திற்குரிய வகையில் செயல்படுகிறது" பகுதியினைப் பரிந்துரைக்கின்றோம்.

நீங்கள் என்ன செய்ய விரும்புகிறீர்கள்?

- [சந்தேகத்திற்கிடமான முறையில் செயல்படும் சாதனத்திற்கான பணிப்பாய்வுக்கு அழைத்துச் செல்லுங்கள்](../../../device-acting-suspiciously)

- [இங்கே அடுத்த படிக்கு என்னை அழைத்துச் செல்லுங்கள்](#முன் மூடுதல்)

### பாதுகாப்பு-விழிப்பூட்டல்கள்-அறிமுகம்

> மின்னஞ்சல் சேவைகள், சமூக வலைப்பின்னல் தளங்கள் அல்லது நீங்கள் உண்மையில் பயன்படுத்தும் வேறு ஏதேனும் ஆன்லைன் சேவையிலிருந்து நீங்கள் செய்திகள் அல்லது அறிவிப்பு விழிப்பூட்டல்களைப் பெறுகிறீர்கள் என்றால், மேலும் அவை புதிய சாதனங்கள் அல்லது இருப்பிடங்களிலிருந்து புதிய சந்தேகத்திற்கிடமான உள்நுழைவுகள் போன்ற பாதுகாப்புச் சிக்கல்களுடன் தொடர்புடையதாக இருந்தால், முதலில் நீங்கள் செய்தியை முறையானதா அல்லது தகவல் திருட்டுடன் தொடர்புடையதா என்பதனை உறுதிப்படுத்திக்கொள்ளலாம். மேற்கொண்டு செல்வதற்கு முன்னர் இதைச் செய்ய, டிஜிட்டல் முதலுதவி பொதியின் பணிப்பாய்வு [எனக்கு சந்தேகத்திற்கிடமான செய்தி கிடைத்தது](../../../suspicious-messages) பரிசீலிக்க பரிந்துரைக்கிறோம்.

>

> செய்தி சட்டப்பூர்வமானதாக இருந்தால், இந்தச் செய்தி சட்டப்பூர்வமானதாக இருப்பதற்கான காரணம் உள்ளதா என்பது நீங்கள் வினவ வேண்டிய அடுத்த வினாவாகும். உதாரணமாக, நீங்கள் VPN சேவை அல்லது Tor ஐப் பயன்படுத்தி, சேவையின் இணையப் பதிப்பிற்குச் சென்றால், நீங்கள் உங்கள் VPN சேவையகம் அல்லது Tor வெளியேறும் முனையின் நாட்டில் இருப்பதாக நினைக்கும், இது ஒரு புதிய சந்தேகத்திற்கிடமான உள்நுழைவு பற்றிய எச்சரிக்கையைத் தூண்டும். அது நீங்கலாகக் காணப்படுகின்ற வேளையில் ஒரு புறக்கணிக்கின்ற தீர்வினை பயன்படுத்தலாம்.

>

> நமக்கு நாமே கேட்டுக்கொள்ள வேண்டிய மற்றொரு பயனுள்ள விஷயம் என்னவென்றால், நாங்கள் எந்த வகையான பாதுகாப்பு விழிப்பூட்டலைப் பெறுகிறோம்: இது உங்கள் கணக்கில் யாரேனும் உள்நுழைய முயற்சிப்பது பற்றியா அல்லது அவர்கள் வெற்றி பெறுகிறார்களா? வருகின்ற பதிலினடிப்படையில் தேவைப்படுகின்ற பிரதிபலிப்பானது வேறுபட்டனவாகக் காணப்படலாம்.

>

> தோல்வியுற்ற உள்நுழைவு முயற்சிகள் பற்றிய அறிவிப்பைப் பெற்றிருந்தால், எங்களிடம் நல்ல கடவுச்சொல் காணப்பட்டு (நீண்டது, பிற பாதுகாப்பற்ற சேவைகளுடன் பகிரப்படவில்லை போன்றவை) மற்றும் பல காரணி உறுதிப்படுத்தல்களினை பயன்படுத்தினால் (MFA அல்லது 2FA என்றும் அழைக்கப்படுகிறது), கணக்கினை பறிகொடுத்தல் தொடர்பாக நாங்கள் கவலைப்பட வேண்டிய அவசியமில்லை. கணக்கு தாக்கப்படுவதற்கான அச்சுறுத்தல் எவ்வளவு தீவிரமானது என்பதைப் பொருட்படுத்தாமல், இருப்பிடம் மற்றும் சாதனத்தின் வகை உட்பட, எங்கள் உள்நுழைவு வரலாற்றை வழக்கமாக மதிப்பாய்வு செய்யக்கூடிய சமீபத்திய செயல்பாடுகளில் ஏதேனும் பதிவுகளைச் பரிசீலிப்பது எப்போதும் நல்லது.

>

> உங்கள் செயல்பாட்டுப் பதிவுகளில் ஏதேனும் சந்தேகத்திற்குரியதாகக் காணப்பட்டால், கணக்கைப் பொறுத்து, மிகவும் பொதுவான உத்திகளில் பின்வருவன அடங்கும்:

>

> - கடவுச்சொற்களை மாற்றுதல்

> - MFA ஐ இயக்குதல்

> - கணக்கிலிருந்து எல்லா சாதனங்களையும் துண்டிக்க முயற்சித்தல்.

> - ஹேக்கிங் முயற்சியின் அறிகுறிகளினை ஆவணப்படுத்தல் (நாம் உதவி தேட விரும்பினால், மேலும் விசாரிக்க அல்லது சட்ட நடவடிக்கையைத் தொடங்க விரும்பினால்)

>

> இந்த அறிவிப்புகளை மதிப்பிட உதவும் மற்றொரு முக்கியமான கேள்வி என்னவென்றால், விழிப்பூட்டலைத் தூண்டிய வேறு ஒருவருடன் சாதனங்களைப் பகிர்ந்தோ அல்லது கணக்கிற்கான அணுகலையோ பகிர்ந்தால். இதுபோன்றால், உங்கள் தகவலுக்கு மற்றவர்களுக்கு நீங்கள் வழங்கும் அணுகல் அளவைக் குறித்து கவனமாக இருக்கவும், இந்த மூன்றாம் நபருக்கான அணுகலைத் திரும்பப் பெற விரும்பினால், மேலே உள்ள படிகளை மீண்டும் செய்யவும்.

>

பணிப்பாய்வுகளின் தொடக்கத்தில் பட்டியலிடப்பட்ட பிற சாத்தியமான அச்சுறுத்தல்கள் உள்ளன என்று நீங்கள் நம்பினால், அல்லது மிகவும் சிக்கலான வழக்கு இருந்தால், மேலும் உதவியைத் தேட விரும்பினால், அடுத்து என்பதைக் கிளிக் செய்யவும்.

- [அடுத்து](#முன் மூடுதல்)

### சந்தேகத்திற்கிடமான-சாதனம்-அறிமுகம்

> சந்தேகத்திற்கிடமான சாதனம் கண்டுபிடிக்கப்பட்டால், முதலில் நம்மை நாமே கேட்டுக்கொள்ள வேண்டியது இந்த சாதனம் தீங்கிழைக்கிறதா அல்லது அது இருக்கும் இடத்தில் இருக்க வேண்டுமா என்பதுதான். ஏனென்றால், கடந்த ஆண்டுகளில் நமது வீடுகள் மற்றும் பணியிடங்களில் தகவல் தொடர்பு திறன் கொண்ட சாதனங்களின் எண்ணிக்கை கணிசமாக வளர்ந்துள்ளது: பிரிண்டர்கள், ஸ்மார்ட் லைட்டுகள், வாஷிங் மெஷின்கள், தெர்மோஸ்டாட்கள் போன்றவை. இந்தச் சாதனங்களின் எண்ணிக்கையைக் கருத்தில் கொண்டு, நாம் கவலைப்பட வேண்டியிருக்கும். அமைப்பது எங்களுக்கு நினைவில் இல்லாத அல்லது வேறொருவரால் உள்ளமைக்கப்பட்ட சாதனம், ஆனால் தீங்கிழைக்கும் சாதனம் அல்ல.

>

> நீங்கள் கண்டறிந்த சாதனம் தீங்கிழைக்கும் சாதனமா என்று உங்களுக்குத் தெரியாவிட்டால், முதலில் செய்ய வேண்டிய ஒன்று அதைப் பற்றிய தகவலைப் பெறுவது: பிராண்ட், மாடல், அது வயர்டு நெட்வொர்க்குடன் அல்லது வயர்லெஸ் ஒன்றுடன் இணைக்கப்பட்டிருந்தால் அது என்ன செய்கிறது, இயக்கப்பட்டிருந்தால், முதலியன

சாதனத்தை மதிப்பாய்வு செய்த பிறகு, அது முறையானது என்று நினைக்கிறீர்களா?

- [இது ஒரு முறையான சாதனம்](#முன் மூடுதல்)

- [நான் சோதித்தேன், ஆனால் சாதனம் என்ன செய்கிறது அல்லது அது தீங்கிழைக்கிறதா என்று இன்னும் தெரியவில்லை](#சந்தேகத்திற்குரிய சாதனம்2)

### சந்தேகத்திற்கிடமான சாதனம்2

> ஆரம்ப மதிப்பாய்விற்குப் பிறகும் சாதனத்தைப் பற்றி நீங்கள் கவலைப்படுகிறீர்கள் என்றால், அது ஒரு கண்காணிப்புச் சாதனமாக இருப்பதற்கான தொலை சாத்தியத்தை நீங்கள் கருத்தில் கொள்ள வேண்டும். வழக்கமாக இந்தச் சாதனங்கள் தாங்கள் இணைக்கப்பட்ட பிணையத்தில் செயல்பாட்டைக் கண்காணிக்கலாம் அல்லது ஸ்பைவேரைப் போலவே ஆடியோ மற்றும்/அல்லது வீடியோவைப் பதிவுசெய்து அனுப்பலாம். இந்த சூழ்நிலை மிகவும் அசாதாரணமானது மற்றும் பொதுவாக அதிக ஆபத்துள்ள சுயவிவரங்களுடன் இணைக்கப்பட்டுள்ளது என்பதைப் புரிந்துகொள்வது அவசியம். இருப்பினும், இது உங்களைப் பற்றியதாக இருந்தால், நீங்கள் செய்யக்கூடிய சில விஷயங்கள் பின்வருமாறு:

>

> - நெட்வொர்க்/பவர் ஆகியவற்றிலிருந்து சாதனத்தைத் துண்டித்து, சுற்றியுள்ள அனைத்து உத்தேசிக்கப்பட்ட சேவைகளும் சிக்கல்கள் இல்லாமல் செயல்படுகின்றனவா என்பதைச் சரிபார்க்கவும். அதன் பிறகு, அனுபவமுள்ள ஒருவரால் சாதனத்தை பகுப்பாய்வு செய்யலாம்.

> - இன்னும் சிலவற்றை ஆராய்ந்து உதவி தேடுதல் (இது பொதுவாக நெட்வொர்க்கை மேப்பிங் செய்வது அல்லது அசாதாரணமான சிக்னல்களைத் தேடுவது போன்ற மேம்பட்ட சோதனைகளை உள்ளடக்கியது).

> - VPN, Tor அல்லது உங்கள் இணைய உலாவல் மற்றும் தகவல்தொடர்பு போன்றவற்றை குறியாக்கம் செய்யும் கருவியைப் பயன்படுத்தி சாதனத்தை இணைக்கும்போது, ​​நெட்வொர்க்கின் கண்காணிப்பைத் தணிக்க ஒரு தடுப்பு நடவடிக்கையாக

இறுதி முதல் இறுதி குறியாக்கத்துடன் கூடிய கருவிகள்.

> - சாதனத்தை இணைப்பில் விட்டுவிட்டால், சாத்தியமான ஆடியோ/வீடியோ பதிவைத் தணிக்க ஒரு தடுப்பு நடவடிக்கையாக, சாதனத்தை பௌதீக ரீதியாக தனிமைப்படுத்தி, அது மதிப்புமிக்க ஆடியோ அல்லது வீடியோவைப் பிடிக்காது.

ஆரம்பத்தில் பட்டியலிடப்பட்டுள்ள பிற சாத்தியமான அச்சுறுத்தல்கள் இருப்பதாக நீங்கள் நம்பினால், நீங்கள் சரிபார்க்க விரும்பினால் அல்லது உதவி தேட விரும்பினால், அடுத்து என்பதைக் கிளிக் செய்யவும்.

- [அடுத்து](#முன் மூடுதல்)

- [எனது பிரச்சினைகளை நான் தீர்த்துவிட்டேன் என்று நினைக்கிறேன்](#தீர்ந்தது\_முடிவு)

### கசிந்த-இணைய-தகவல்-அறிமுகம்

> இந்த பணிப்பாய்வு பிரிவு இணைய சேவைகள் மற்றும் செயல்பாட்டிலிருந்து கசிந்த தரவை உள்ளடக்கும். தொலைபேசி தொடர்புகளிலிருந்து கசிந்த தகவல்களுக்கு, ["தொலைபேசி அழைப்புகள் அல்லது எஸ்எம்எஸ் மூலம் பகிரப்பட்ட ரகசியத் தகவல் எதிரிக்கு கசிந்ததாகத் தெரிகிறது"](#லீக்-ஃபோன்-இன்போ-அறிமுகம்) என்ற பகுதியைப் பார்க்கவும்.

>

> பொதுவாக, இணைய அடிப்படையிலான சேவைகளில் இருந்து கசிவுகள் மூன்று காரணங்களால் நிகழலாம்:

>

> 1. தகவல் முதலில் பொதுவில் இருந்தது, இது இந்த ஆதாரத்தில் இடம்பெறாது.

> 2. கணக்கில் இருந்து தகவல் நேரடியாக கசிந்தது (பாதிக்கப்பட்டவருக்கு நெருக்கமான "சிறிய" எதிரிகளுக்கு மிகவும் பொதுவானது).

> 3. தகவல் முதலில் பதிவேற்றப்பட்ட மேடையில் இருந்து கசிந்தது (அரசாங்கங்கள் மற்றும் பெரிய நிறுவனங்கள் போன்ற "பெரிய" எதிரிகளுக்கு மிகவும் பொதுவானது).

>

> கடந்த இரண்டு நிகழ்வுகளை உள்ளடக்குவோம், ஏனெனில் அவை குடிமை விண்வெளி சமூகத்தில் காணப்படும் பொதுவான அவசரநிலைகளுடன் தொடர்புடையவை. கீழே உள்ள கேள்வியிலிருந்து நீங்கள் பணிப்பாய்வுகளைப் பின்பற்றலாம்:

உங்கள் எதிரியுடன் சாதனங்கள் அல்லது கணக்குகளைப் பகிர்கிறீர்களா?

- [ஆம்](#பகிரப்பட்ட சாதனங்கள் அல்லது கணக்குகள்)

- [இல்லை](#லீக்-இன்டர்நெட்-தகவல்2)

### பகிர்ந்த சாதனங்கள் அல்லது கணக்குகள்

> சில சந்தர்ப்பங்களில், பிறருடன் கணக்கு அணுகலைப் பகிர்வது, திட்டமிடப்படாத தரப்பினருக்கு முக்கியமான தகவல்களை அணுகலாம், பின்னர் அவை எளிதில் கசிந்துவிடும். மேலும், பொதுவாக நாம் கணக்குகளைப் பகிரும் போது, ​​இந்த செயல்முறையை நடைமுறைக்குக் கொண்டு வர வேண்டும், இது பெரும்பாலும் கணக்கு அணுகல் வழிமுறைகளின் பாதுகாப்பைப் பாதிக்கிறது, கடவுச்சொற்களை எளிதாகப் பகிரும் வகையில் பலவீனமாக்குவது மற்றும் பலர் உள்நுழைய அனுமதிக்கும் பல காரணி அங்கீகாரத்தை (MFA அல்லது 2FA) முடக்குவது போன்றவை. அதே கணக்கில்.

>

> ஒரு முதல் ஆலோசனையானது, தொடர்புடைய கணக்குகள் அல்லது ஆதாரங்களை (கிளவுட் ஸ்டோரேஜில் உள்ள ஆவணங்கள் போன்றவை) யார் அணுக வேண்டும் என்பதை மதிப்பிடுவது மற்றும் முடிந்தவரை குறைவான நபர்களுக்கு மட்டுமே. மற்றொரு பயனுள்ள கொள்கை, ஒவ்வொரு நபருக்கும் ஒரு கணக்கை வைத்திருப்பது, ஒவ்வொருவரும் தங்கள் அணுகல் அமைப்புகளை மிகவும் பாதுகாப்பான முறையில் உள்ளமைக்க அனுமதிக்கிறது.

>

> ["நம்பகமான சேவைகளில் இருந்து பாதுகாப்புச் செய்திகள் மற்றும் விழிப்பூட்டல்களைப் பெறுகிறேன்"](#security-alerts-intro) என்ற பகுதியைச் சரிபார்க்கவும் பரிந்துரைக்கப்படுகிறது, அங்கு சந்தேகத்திற்குரிய அணுகல் ஏற்பட்டால் கணக்குகளை கடினப்படுத்துவதற்கான உதவிக்குறிப்புகளைக் காணலாம்.

உங்கள் நிலைமையை மேலும் விரிவாக ஆராய அடுத்து என்பதைக் கிளிக் செய்யவும்.

- [அடுத்து](#லீக்-இன்டர்நெட்-தகவல்2)

### கசிந்த-இணைய-தகவல்2

நீங்கள் பயன்படுத்தும் ஆன்லைன் சேவைகளை உங்கள் எதிரியால் கட்டுப்படுத்த முடியுமா அல்லது அணுக முடியுமா மற்றும் கசிந்த தகவலை சேமிக்க முடியுமா? (\*இது பொதுவாக அரசாங்கங்கள், சட்ட அமலாக்க முகவர் அல்லது வழங்குநர்களுக்கே பொருந்தும்\*)

- [ஆம்](#ஆன்லைன் சேவைகளின் கட்டுப்பாடு)

- [இல்லை](#லீக்-இன்டர்நெட்-தகவல்3)

### ஆன்லைன் சேவைகளின் கட்டுப்பாடு

> சில நேரங்களில் நாம் பயன்படுத்தும் தளங்கள் எதிரிகளால் எளிதில் அணுகப்படும் அல்லது கட்டுப்படுத்தப்படும். உங்களை நீங்களே கேட்டுக்கொள்ளக்கூடிய சில பொதுவான கேள்விகள்:

>

> - சேவை யாருடையது?

> - இது ஒரு எதிரியா?

> - சட்டரீதியான தரவு விசாரணைகள் மூலம் எதிரிக்கு சர்வர்கள் அல்லது தரவை அணுக முடியுமா?

>

> அப்படியானால், எதிர்காலத்தில் கசிவுகளைத் தவிர்க்க, எதிரியால் கட்டுப்படுத்தப்படாத வேறு தளத்திற்கு தகவலை நகர்த்துவது நல்லது.

>

> பிற பயனுள்ள குறிகாட்டிகள் இருக்கலாம்:

>

> - உள்நுழைவு செயல்பாடு (புவியியல் இருப்பிடங்கள் உட்பட), இருந்தால்

> - படித்த மற்றும் படிக்காத கூறுகளின் விசித்திரமான நடத்தை

> - உள்ளமைவுகள், செய்திகள் அல்லது தகவல்களுக்கு என்ன செய்ய வேண்டும் என்பதைப் பாதிக்கிறது.

>

> கேனரி டோக்கன்களைப் பயன்படுத்தி உங்களின் செய்திகளை யாரேனும் விரும்பாமல் படிக்கிறார்களா என்பதை நீங்கள் சரிபார்க்கலாம், அதாவது [canarytokens.org](https://canarytokens.org/generate)

உங்கள் நிலைமையை மேலும் விரிவாக ஆராய NEXT என்பதைக் கிளிக் செய்யவும்.

- [Next](#leaked-internet-info3)

### கசிந்த-இணைய-தகவல்3

உங்கள் எதிரிக்கு கண்காணிப்பு உபகரணங்களுக்கான அணுகல் மற்றும் அதை உங்களுக்கு அருகில் நிலைநிறுத்தும் திறன் உள்ளதா?

- [ஆம்](#லீக்-இன்டர்நெட்-தகவல்4)

- [இல்லை](#முன் மூடுதல்)

### கசிந்த-இணைய-தகவல்4

> மிகவும் சக்திவாய்ந்த எதிரிகள், தங்களின் பாதிக்கப்பட்டவர்களைச் சுற்றி, கண்காணிப்பு சாதனங்களை நடுதல் அல்லது ஸ்பைவேர் மூலம் உங்கள் சொந்த சாதனங்களைப் பாதிப்பது போன்ற சிறப்புக் கண்காணிப்பு உபகரணங்களைப் பயன்படுத்துவதற்கான திறனைக் கொண்டிருக்கலாம்.

கண்காணிப்பு சாதனம் மூலம் நீங்கள் கண்காணிக்கப்படலாம் அல்லது உங்கள் கணினி அல்லது மொபைல் உங்களை உளவு பார்ப்பதற்காக தீம்பொருளால் பாதிக்கப்பட்டிருக்கலாம் என நினைக்கிறீர்களா?

- [சாதனங்களை கண்காணிப்பது பற்றி மேலும் அறிய விரும்புகிறேன்](#tracking-device-intro)

- [எனது சாதனம் தீம்பொருளுடன் சமரசம் செய்யப்படுவதற்கான சாத்தியக்கூறுகள் பற்றி மேலும் அறிய விரும்புகிறேன்](#device-behaviour-intro)

### கசிந்த தொலைபேசி-தகவல்-அறிமுகம்

> இந்த பணிப்பாய்வு அறிமுகத்தில் விவரிக்கப்பட்டுள்ளபடி, பெரும்பாலான (அனைத்தும் இல்லாவிட்டாலும்) பிராந்தியங்கள் மற்றும் நாடுகளில் பாரிய தொலைபேசி கண்காணிப்பு என்பது எங்கும் நிறைந்த அச்சுறுத்தலாகும். அடிப்படைத் தகவலாக, கேரியர்கள் (மற்றும் கட்டுப்பாடு அல்லது அணுகல் உள்ள எவரும்) தகவலைச் சரிபார்ப்பது மிகவும் எளிதானது என்பதை நாங்கள் அறிந்திருக்க வேண்டும்.

இது போன்றது:

>

> - வரலாற்று இடம் (ஒவ்வொரு முறையும் ஃபோன் ஆன் மற்றும் நெட்வொர்க்குடன் இணைக்கப்பட்டிருக்கும்), மொபைல் ஃபோன் டவர்களில் உள்ள தரவு, ஃபோன் இணைக்கப்பட்டிருக்கும்

> - அழைப்பு பதிவுகள் (யார் யாரை, எப்போது, ​​எவ்வளவு நேரம் அழைக்கிறார்கள்)

> - SMS (பதிவுகள் மற்றும் செய்திகளின் உண்மையான உள்ளடக்கம் இரண்டும்)

> - இன்டர்நெட் டிராஃபிக் (இது குறைவான பொதுவானது மற்றும் எதிரிகளுக்குப் பயன்படுவது குறைவு, ஆனால் எந்தெந்த பயன்பாடுகள் எப்போது பயன்படுத்தப்படுகின்றன, எந்த இணையதளங்கள் ஆலோசிக்கப்படுகின்றன, முதலியன இதில் இருந்து ஊகிக்க முடியும்.)

>

> சில சூழல்களில் இன்னும் கவனிக்கப்படும் மற்றொரு காட்சி, அசாதாரணமானது என்றாலும், ஸ்டிங்ரேஸ் அல்லது IMSI-கேட்சர்கள் எனப்படும் பௌதீக இடைமறிப்பு சாதனங்களின் பயன்பாடு ஆகும். இந்தச் சாதனங்கள் ஒரு முறையான செல் நெட்வொர்க் கோபுரத்தைப் போல ஆள்மாறாட்டம் செய்து, அவற்றின் மூலம் நெருங்கிய பௌதீக பகுதியில் உள்ளவர்களின் ஃபோன் டிராஃபிக்கைத் திருப்பிவிடுகின்றன. இந்தச் சாதனங்களைச் செயல்படுத்தும் பாதிப்புகள் புதிய நெறிமுறைகள் (4G/5G) மூலம் தீர்க்கப்படும் அல்லது குறைக்கப்படும்போது, ​​கிடைக்கக்கூடிய ஒரே நெறிமுறை 2G (இந்தச் சாதனங்களால் மிகவும் பரவலாகப் பயன்படுத்தப்படும்) நெறிமுறைகள் என்று ஃபோன்கள் நம்புவதற்கு சிக்னலை முடக்குவது இன்னும் சாத்தியமாகும். இந்த விஷயத்தில், சில நம்பகத்தன்மையுடன் சில குறிகாட்டிகள் உள்ளன, குறிப்பாக 4G அல்லது 5G இருக்க வேண்டிய பகுதிகள் அல்லது மற்றவர்கள் புதிய நெறிமுறைகளுடன் எந்த பிரச்சனையும் இல்லாமல் இணைக்கப்பட்டுள்ள இடங்களில் 2G க்கு "தரமிறக்கப்பட்டது". மேலும் தகவலுக்கு, நீங்கள் [FADe திட்ட இணையதளம்](https://fadeproject.org/?page\_id=36) பார்க்கவும். மேலும், உங்கள் எதிரி இந்த வகையான சாதனத்திற்கான அணுகலை நிரூபித்திருக்கிறாரா என்று நீங்களே கேட்டுக்கொள்ளலாம்.

>

> இந்தக் காட்சிகளுக்கான பொதுவான பரிந்துரையாக, ஆபத்தில் உள்ள நபர்கள் வழக்கமான தொலைபேசி அழைப்புகள் மற்றும் SMSகளுக்குப் பதிலாக இணையத்தை நம்பியிருக்கும் மறைகுறியாக்கப்பட்ட சேனல்களுக்கு தகவல்தொடர்புகளை மாற்றுவது நல்லது. முக்கிய இணைய போக்குவரத்திற்கு (பயன்பாடுகள் உட்பட) VPN அல்லது Tor ஐப் பயன்படுத்துவதைப் போலவே. பெரிய தீர்க்கப்படாத அம்சம் பயனர் இருப்பிடத்தைக் கண்காணிப்பதாகும், இது தொலைபேசி நெட்வொர்க்குடன் இணைந்திருக்கும் போது தவிர்க்க முடியாதது.

>

> கேரியர்கள் மூலம் பாரிய தரவு சேகரிப்பு தொடர்பாக, சில அதிகார வரம்புகளில் பயனர்கள் கடந்த காலத்தில் தங்களைப் பற்றிய எந்தத் தரவு பகிரப்பட்டது என்று கோரலாம். இது உங்களுக்குப் பொருந்துமா மற்றும் சாத்தியமான கண்காணிப்பைக் கண்டறிய அந்தத் தகவல் நம்பகமானதா என்பதை நீங்கள் ஆராயலாம். இது வழக்கமாக ஒரு சட்ட விசாரணையை உள்ளடக்கியது என்பதை நினைவில் கொள்ளவும்.

நீங்கள் பிற சாத்தியமான அச்சுறுத்தல்களைச் சரிபார்க்க விரும்பினால் அல்லது மிகவும் சிக்கலான வழக்கு இருந்தால், உதவியைத் தேட விரும்பினால், அடுத்து என்பதைக் கிளிக் செய்யவும்.

- [அடுத்து](#முன் மூடுதல்)

### சகபாடிகள் -தாக்கப்படுத்தல் -அறிமுகம்

> உங்களுடன் தொடர்புடைய எந்தவொரு நபரும் அல்லது நிறுவனமும் கண்காணிப்புக்கு பலியாகியிருந்தால், அவர்களில் பயன்படுத்தப்பட்ட நுட்பங்களைப் புரிந்துகொள்ள முயற்சிக்குமாறு பரிந்துரைக்கிறோம், மேலும் முந்தைய பட்டியலில் நெருக்கமானவற்றைத் தேர்ந்தெடுக்கவும், எனவே நீங்கள் மிகவும் பொருத்தமான சூழலைப் பெறலாம் மற்றும் நீங்களும் இதே போன்ற நுட்பங்களுக்கு பலியாகலாமா என்று முடிவு செய்யுங்கள்.

நீங்கள் என்ன செய்ய விரும்புகிறீர்கள்?

- [என்னை முந்தைய படிக்கு அழைத்துச் செல்லுங்கள்](#தொடக்கம்)

- [எனக்கு உறுதியாக தெரியவில்லை](#முன் மூடுதல்)

### மற்ற அறிமுகம்

> நீங்கள் முன்பு பார்த்த பட்டியலில் உதவியாளர்களால் சிவில் இடத்தில் காணப்பட்ட பொதுவான நிகழ்வுகள் சேர்க்கப்பட்டுள்ளன, ஆனால் உங்கள் நிலைமை அங்கு குறிப்பிடப்படாமல் இருக்கலாம். அது உங்கள் வழக்கு என்றால், "எனக்கு உதவி தேவை" என்பதைக் கிளிக் செய்யவும்; இல்லையெனில், நீங்கள் மிகவும் பொதுவான நிகழ்வுகளின் பட்டியலுக்குச் சென்று, மேலும் குறிப்பிட்ட வழிகாட்டுதலைப் பெற உங்களுக்குப் பொருந்தக்கூடிய நெருக்கமான சூழ்நிலையைத் தேர்ந்தெடுக்கலாம்.

நீங்கள் என்ன செய்ய விரும்புகிறீர்கள்?

- [சாத்தியமான அச்சுறுத்தல்களின் பட்டியலுக்கு என்னை அழைத்துச் செல்லுங்கள்](#தொடக்கம்)

- [எனக்கு உதவி தேவை](#உதவி\_முடிவு)

### முன் மூடல்

> இந்த பணிப்பாய்வு இதுவரை உதவியாக இருந்ததாக நம்புகிறோம். நீங்கள் கவலைப்படக்கூடிய பிற அச்சுறுத்தல்களைச் சரிபார்க்க, காட்சிகளின் ஆரம்பப் பட்டியலுக்குச் செல்ல நீங்கள் தேர்வு செய்யலாம் அல்லது மிகவும் சிக்கலான நிகழ்வுகளில் உங்களுக்கு உதவ நீங்கள் தொடர்புகொள்ளக்கூடிய நிறுவனங்களின் பட்டியலுக்குச் செல்லவும்.

நீங்கள் என்ன செய்ய விரும்புகிறீர்கள்?

- [மற்ற கண்காணிப்பு நுட்பங்களைப் பற்றி அறிய விரும்புகிறேன்](#தொடக்கம்)

- [எனது தேவை இந்தப் பிரிவில் இல்லை அல்லது மிகவும் சிக்கலானது என்று நினைக்கிறேன்](#உதவி\_முடிவு)

- [எனக்கு என்ன நடக்கிறது என்பது பற்றி எனக்கு தெளிவான யோசனை இருப்பதாக நான் நினைக்கிறேன்](#தீர்க்கப்பட்ட\_முடிவு)

### உதவி\_முடிவு

> கண்காணிப்பு வழக்குகளைக் கையாள்வதில் கூடுதல் உதவி தேவைப்பட்டால், கீழே பட்டியலிடப்பட்டுள்ள நிறுவனங்களைத் தொடர்புகொள்ளலாம்.

>

> \*குறிப்பு: உதவிக்காக நீங்கள் எந்த நிறுவனத்தையும் தொடர்பு கொள்ளும்போது, ​​இங்கு நீங்கள் பின்பற்றிய பாதையையும், அடுத்த கட்டத்தை எளிதாக்க நீங்கள் கண்டறிந்த எந்த குறிகாட்டியையும் பகிர்ந்து கொள்ளுங்கள்.\*

:[](organisations?services=legal&services=vulnerabilities\_malware&services=forensic)

### சட்ட\_முடிவு

> உங்களை சட்டவிரோதமாக உளவு பார்த்ததற்காக யாரேனும் ஒருவர் மீது வழக்குத் தொடர உங்களுக்கு ஆதரவு தேவைப்பட்டால், கீழே உள்ள நிறுவனங்களில் ஒன்றைத் தொடர்புகொள்ளலாம்.

:[](organisations?services=legal)

### தீர்க்கப்பட்ட\_முடிவு

இந்த சரிசெய்தல் வழிகாட்டி பயனுள்ளதாக இருந்தது என்று நம்புகிறேன். தயவுசெய்து கருத்து தெரிவிக்கவும் [மின்னஞ்சல் வழியாக](mailto:incoming+rarenet-dfak-8220223-issue-@incoming.gitlab.com)

### இறுதி\_உதவிக்குறிப்புகள்

- தொலைபேசி அழைப்புகள் மற்றும் எஸ்எம்எஸ் போன்ற பாதுகாப்பற்ற ஊடகங்களிலிருந்து ஒரு அந்தம் முதல் மாரு அந்தம் வரை மறைக்குறியாக்கம் செய்யப்பட்ட மெசஞ்சர் செயலி மற்றும் HTTPP மூலம் பாதுகாக்கப்பட்ட இணையதளங்கள் போன்ற இணையத்தை நம்பியிருக்கும் மறைக்குறியாக்கம் செய்யப்பட்ட தகவல்தொடர்பு ஊடகங்களுக்கு எந்த தகவல்தொடர்புகளையும் மாற்றவும்.

- உங்கள் இணைய ட்ராஃபிக் கண்காணிக்கப்படுவதாக நீங்கள் அஞ்சினால், இது ஒரு பாதுகாப்பு அச்சுறுத்தலாகக் காணப்பட முடியுமென நீங்கள் நம்பினால், VPN அல்லது Tor போன்ற என்க்ரிப்ஷன் கருவி மூலம் இணையத்துடன் இணைக்கவும்.

- உங்கள் கட்டுப்பாட்டிலுள்ள உள்ள அனைத்து சாதனங்களையும், குறிப்பாக இணையத்துடன் இணைக்கப்பட்டவை, மற்றும்

அவர்கள் என்ன செய்கின்றன என்பதை அறிய முயற்சி செய்யுங்கள்.

- எதிரியால் கட்டுப்படுத்தப்படும் சேவை மூலம் முக்கியமான தகவல்களைப் பகிர்வதைத் தவிர்க்கவும்.

- உங்களால் முடிந்தவரை உங்கள் கணக்குகள் அல்லது சாதனங்களைப் பகிர்வதைக் குறைக்கவும்.

- சந்தேகத்திற்கிடமான செய்திகள், இணையதளங்கள், பதிவிறக்கங்கள் மற்றும் பயன்பாடுகள் குறித்து எச்சரிக்கையாக இருங்கள்.

#### வளங்கள்

- [Apple’s Android App to Scan for AirTags is a Necessary Step Forward, But More Anti-Stalking Mitigations Are Needed](https://www.eff.org/es/deeplinks/2021/12/apples-android-app-scan-airtags-necessary-step-forward-more-anti-stalking).

- [Privacy for Students](https://ssd.eff.org/module/privacy-students): With references of surveillance techniques in schools that can apply to many other scenarios.

- [Security in a Box: Protect the privacy of your online communication](https://securityinabox.org/en/communication/private-communication/)

- [Security in a Box: Visit blocked websites and browse anonymously](https://securityinabox.org/en/internet-connection/anonymity-and-circumvention/)

- [Security in a Box: Recommendations for encrypted chat tools](https://securityinabox.org/en/communication/tools/#more-secure-text-voice-and-video-chat-applications)